girls who code

AT HOME

Cyber Detective

Unplugged Activity

Updated: May 2025

Activity Overview

Did you know that the first smartphone was created in 1992? Even though the Simon phone was considered a “smartphone”, the functions and look of this phone was very basic compared to the phones we use today. Take a look at the photo on the right comparing the Simon phone with an iPhone 4S!

Image Source: Time

The Simon phone contained a touchscreen that could only be used to contain notes, an address book, calendar, clock, and take calls. You can watch this **video** to see a demo of this phone.Technology has evolved exponentially since the first smartphone with almost all types of electronic devices connected to the internet through **WiFi** or **5G**. With the convenience of all of our devices connected comes large potential security risks.

You may be thinking, why is this important? If you purchase items online, fill out a college application, or sign up for a new app you provide sensitive information like a credit card number, your name, your birthday, and sometimes your social security number. In 2019 about 1 in 15 people became victims of **identity fraud**. The first step in protecting yourself is to be educated in the types of attacks that might leave yourself vulnerable. Cybersecurity Specialists are responsible for implementing security measures in any computer (that is any electronic device that is connected to the internet), and recognizing potential threats. In this unplugged activity you will play the role of a cybersecurity specialist, or cyber detective, to follow the clues presented in the story to identify the cyber attack.

Learning Goals

By the end of this activity you will be able to...

- ❏ identify different types of common viruses and cyber attacks.

Materials

- ➔ No additional materials needed

Prior Knowledge

- ➔ No prior knowledge needed!

GWC Tech Spotlight: Jaya Baloo

Image Source: Intelligent CISO

In 2017, Jaya Baloo was named one of the **top 100 CISO** (Chief Information Security Officer). She is an expert in **cryptography**, studying techniques to secure communication. Jaya has been interested in computers since she was 9 years old! After graduating from **Tufts University**, Jaya worked for Bankers Trust as an Internet Security Trainer. It was through this experience that she became aware that cybersecurity was viewed as a weapon by the US, explaining why the US hid their technology from the public. However, Jaya had a different view, cybersecurity should be made publicly available to defend the lives of all.

With the evolution of technology and invention of more "smart" devices, cybersecurity is more important than ever. With all devices connected under one system many people can be left vulnerable to cyber attacks. Jaya now works for **Avast** to bring free antivirus software for all. As part of her work with Avast she works to implement **quantum computing** and **artificial intelligence** to detect threats and secure computers. She believes that cybersecurity is a *fundamental right* and should be freely available.

Watch this **video** to learn more about the importance of cybersecurity and how systems can be easily hacked through connected 5G devices. Want to learn more about Jaya? Watch her **TED talk** in 2017 about how cybersecurity affects our everyday lives and explore her **profile** on Singularity University.

Reflect

Being a computer scientist is more than just being great at coding. Take some time to reflect on how Jaya and her work relates to the strengths that great computer scientists focus on building - bravery, resilience, creativity, and purpose.

PURPOSE

Jaya believes that cybersecurity software should be freely available instead of a paid service. This contrasts to how the US government views this knowledge. What are the benefits for distributing cybersecurity software for free? What are some potential risks for distributing software for free?

Share your responses with a family member or friend. Encourage others to read more about Jaya to join in the discussion!

Step 1: What is Cybersecurity? (2-3 mins)

Imagine a hacker. What do they look like? What do they do? From watching some movies you might imagine a man in a black hoodie in front of a lot of computers. Did you know that about 20% of hackers are women? A **hacker** is someone who uses their computer programming knowledge to expose potential vulnerabilities in a computer system. While you may think a hacker is a bad person, many hackers actually work to defend computers and strengthen security measures against cyber criminals. This practice is called **cybersecurity.**

Cybersecurity is the practice of defending computers (any electronic device that can store and process data), servers, network, and data in general from cyber attacks. With almost all types of electronic devices connected to the internet through WiFi or 5G protecting our information from cyber attacks is more important than ever. You may already be familiar with some famous attacks stemming from privacy leaks of celebrities, information release of sensitive information from governments, to crime shows on TV, or you may personally know someone who has faced a cyber attack.

In 2019 about 1 in 15 people became victims of identity fraud. The first step in protecting yourself is to be educated in the types of attacks that might leave you and your personal data vulnerable. In this activity we will walk you through a few examples of common attacks and give you actionable steps to protect yourself from these potential threats!

Step 2: Review Activity Instructions (2 mins)

In this activity you will be taking on the role of a detective specializing in cyber attacks, or a *cyber detective*. In this choose your own adventure activity you will decide which actions to take to respond to a cyber attack.

In the opening scene of the story you will get some information of what has happened and some clues about the situation. At the end of each scene of the story you will be given two choices in what to do next. Once you select a choice, you will follow the instructions associated with your choice. Instructions will differ depending on each of your choices and will affect the overall outcome of the story. If you don't like the result you got, go back and try the story again!

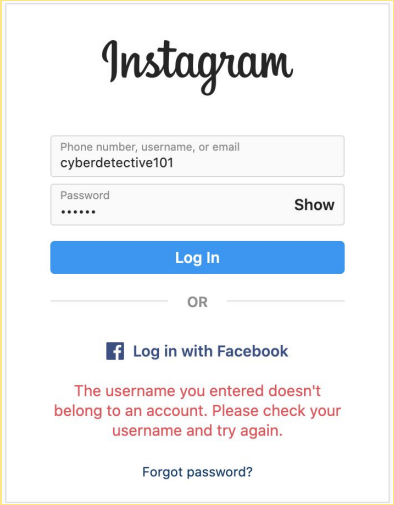
Now that you got a general gist of the instructions for this activity, it is time to put on your detective hat and virtual magnifying glasses and get started!

Parent/Teacher Tip

Want to make this activity more active? We suggest making a mini scavenger hunt out of the scenes and update the instructions for your cyber detective!

Step 3: Read about the Instagram Crisis (10-15 mins)

Just like any normal morning, you wake up, turn on your phone, and immediately open Instagram. As you are slowly rubbing the sleep off your eyes, you notice something different on your screen. After rubbing your eyes a few more times, you see the following message:



The username you entered doesn't appear to belong to an account. Please check your username and try again.

You think, "Hmm, that's weird, maybe I typed in the wrong password?" You try to log in again and you get the same error message. You think, "What does this even mean? I know what my username and password are!!"

What do you do next?

A. Shrug it off, set down your phone and go get ready for school. You will just try to log in again later. **Go to page 6.**

B. **FREAK OUT!** Start Googling the error message to learn more about what to do next. Go to page 7.

Page 6

You start getting ready with your usual morning routine but you have a pit in your stomach telling you something might be wrong. You ignore it for now, it's more important to get ready for school. You get breakfast, say goodbye to your family and head towards the bus stop so you can make your way to school.

While you're on the bus you decide to kill some time and try logging into Instagram again. You enter in your login credentials, this time being extra careful that there are no typos in your username or password. You are still getting the same error, now what?

A. You Google the error message to understand what it means. Go to **page 7.**

B. You assume that there must be something wrong with Instagram and just ignore the message again. You move on to checking your email. Go to **page 9.**

Page 7

You copy and paste the error message into the Google search bar and come across a **Quora question**.

Question: I'm trying to log into Instagram but the site says my username doesn't belong to an account. Does anyone know how to fix this?

Answer: Double-check that you're spelling it correctly. Punctuation, capitalization, spelling, symbols. Everything. Copy and paste if you have to.

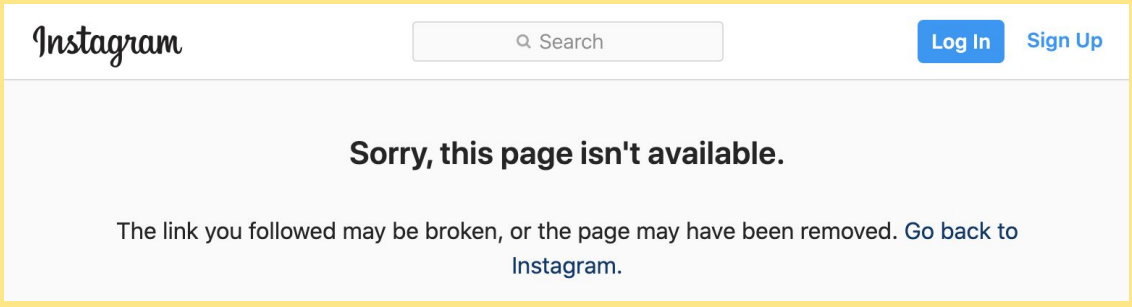
Still not working?

Try logging in with Facebook or Email instead.

Still not working?

Your account may have been disabled or banned (meaning you were reported for violating one or more of Instagram's policy). To see if this is the case, go to a web browser on a computer and type "http://www.instagram.com/[your profile here]" and see if your account pops up. If it doesn't, then you may have been deleted. Make a new account, or contact the Instagram team. If it does, then try the first two options again. Still won't work? Email the Instagram team.

You follow the instructions you found in the Quora answers above. You first try logging in with your credentials, checking yet again that your username and password is spelled correctly. No luck. Still not working. Next, you try logging in with Facebook, *nothing*. Your heart sinks a little, unsure of what this really means. You try the very last step. You open up Safari on your phone and type "**http://www.instagram.com/cyberdetective101**".



"Sorry, this page isn't available"

Turn to the page 8 to continue the story.

Page 8

The last step, secretly you were hoping that you wouldn't have to do the last step. You locate the **HELP** button and look through the topics. You select **Login Troubleshooting** under Popular Topics. You then select "I can't locate my account or don't know my username on Instagram" and read the answer.

If you aren't able to locate your account after entering your username:

- ➔ Make sure that you're entering your username correctly, especially if it contains repeated characters.
- ➔ Don't include the @ symbol when entering your username.

If you think your username was changed as a result of your account being compromised:

- ➔ Check if you've received an email from Instagram notifying you that your account information was changed.
- ➔ Ask a friend to visit your profile and take a screenshot of your current username.

Learn more about what you can do if you **think your account was hacked**.

You try all of these suggestions and look at the last sentence. You think, "was my account hacked?" What do you do next?

A. You think, "Why would anyone even be interested in hacking my account? I don't even have that many followers and my account is private!" You ignore it and decide to just wait until the afternoon to check again. Go to **page 9**.

B. You think, "maybe someone did hack my account." You click the **link** and follow the next steps. Go to **page 10**.

Page 9

As you scan your email, your eye immediately catches an email with a subject line, “Contact us if you want your Instagram account back”. You click to open the email and read the details.

> Hi @cyberdetective101,
>
> We have taken over your account and have gotten access to your photos, friends, and information. If you do not respond by sending over $2,000 to **this account** by tonight, we will delete your account and sell your personal information.
>
> Don’t try to contact Instagram for help because we have successfully changed all of your information and will be alerted if you try to restore your account and instantly delete it.

You can’t believe this is happening! What do you do next?

A. You send the money. Everything should be fine right? Go to **page 11**.

B. You did get hacked! You ignore the message and go straight to the Instagram help page. Go to **page 10**.

Page 10

Going through the Instagram Help page, you come across **I think my Instagram account has been hacked**. You click the link and begin following the steps listed in the Instagram Help information.

You check your email for a message from Instagram. You scan through your email in detail and even check your Trash folder. Sure enough, you noticed an email from Instagram about 2 days ago notifying you that your email address changed. You try to revert the change by clicking the **secure your account here** link**.**

In order to confirm your account you need to verify your identity, but you don't recognize any of the recovery options. The email and phone number has changed on your account.

The only thing left to do is to follow the steps to report the account and hope for the best. You continue to wait for Instagram's reply to your request.

Go to page 12.

Page 11

You quickly pull up your parent's credit card information, thinking to yourself "Phew, I'm so glad mom let me save their card info to my account on the App store!" Card info in hand, you click the link in the email, and follow the instructions to send the money. You breathe a sigh of relief and wait for your account to be returned to you. Finally this nightmare is almost over.

You open a web browser on your phone and you notice this pop up that says.

Your Phone Has Been Hacked!
All Actions on the device are tracked by a hacker.

Immediate Action is Required!

You got a new email. You check it and it is another email from your hacker, it reads:

Hi @cyberdetective101,

We have now taken over your phone and have access to all of your photos, contacts, and information. If you do not respond by sending over $10,000 to **this account** by tonight, we will sell your personal information and contact all of your friends.

Your systems have been hacked and now you run the risk becoming a victim of identity fraud.

Go to page 12.

Step 4: Conclusion (10-15 mins)

Depending on the path you chose throughout the story, you may have been hacked by multiple cyber attacks.

Attack #1: Weak Passwords (5-8 mins)

If a hacker was able to access your account, most likely this is due to a **weak/vulnerable password**. When creating a password there may be some simple requirements before you are able to create a valid account. Some restrictions may include:

- 6-8 minimum characters
- A variety of uppercase and lowercase letters
- At least one number used
- At least one special character

Even if you create a password that meets the minimum requirements, it could take a hacker mere seconds to a day to crack your password! It is extremely simple and cheap for hackers to hack most accounts. Take a look at the chart below to compare how passwords may affect the vulnerability of your online accounts.

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io

Image Source: Reddit

Take a moment to reflect on what you just learned about passwords and experiment on your own to see if you can create secure passwords!

- ❏ **Rank the following passwords from 1-5, where 1 represents the most secure and 5 represents the least secure password.** *In order to help you rank the passwords, we included a few columns: number of characters and character variation.*
  - ❏ **Fill out the # of characters column and character variation for each password.**
  - ❏ **Rank the passwords from 1-5.**
  - ❏ **Check your answers by using this website and type in each option.** Fill out the last column, time for hacker to crack to compare your rankings.

Rank *1: most secure to 5: least secure*	**Password**	**# of characters** *How many characters are in the password?*	**Character Variation** *Does the password include upper and/or lower case letters? Numbers? Symbols?*	**Time for Hacker to Crack** *Based on this website, how long would it take for a hacker to crack the password?*
Example Password	*ku8@}:'$*	*8*	*Lowercase letters, symbols, numbers*	*4 hours*
	hcVESx			
	vWESp3Tt			
	Sg3Jpezyhv			
	password1			
	jG/8ab{s			

❑ Take **2 minutes** to come up with your own secure passwords and write them down in the space below. Your passwords should take *at least 1 year* for hackers to crack.

1.

2.

3.

❑ Navigate to **this website** to check how secure the passwords in the previous steps.

Were you surprised at your results? Here are some general guidelines and recommendations for securing all of your accounts

➔ **Never use the same passwords for multiple accounts.** Some websites are more secure than others, and if a hacker gains access to one account you do not want to make it easier for them to access your other accounts. Remembering all of your various passwords may be difficult, therefore we suggest using a password manager like **BitWarden**, **KeePassXC**, or **LastPass**.

➔ **Never save your password to your browser.** Every time you log into a website online, your browser should ask you if you want to save your password. **Select Never!** Even though it is difficult to remember your passwords, by saving your passwords to the browsers makes it easier for hackers to access your information. Use password managers to help you remember your complex passwords.

➔ **Use a variety of characters in your password.** In general passwords should use a variety of uppercase and lowercase letters, numbers, and special characters and be at least 11 characters in length. You should avoid using typical words like “password”, names, typical dates (like birth dates), or numbers such as “111” or “1234”.

➔ **Set up 2-Factor Authentication (2FA)**. To secure your accounts further turn on 2FA setting which forces to you log into accounts by password **and** verification through a trusted device, email, or security questions. This extra step goes a long way in securing your accounts. Review this **article** to see how to turn on 2FA for a variety of accounts including **Instagram**, **Amazon**, **Facebook**, **Google**, and **Twitter**.

➔ **Change your passwords often.** It is good practice to change your password every three months.

Attack #2: Phishing (5-8 mins)

Phishing is often an email, text message, or pop-up message that appears to be from a well-known source and asks users to click on a link or provide sensitive information. These emails can appear to be from a bank, university credentials, various online accounts, etc. These links often lead users to unsecure websites where attackers may be able to gain access to your computer and continue with other malicious activity.

Sometimes the websites replicate well-known sites and steal your information once you log into their sites.

In our story you may have chosen a path where you received a malicious email. This particular email is different from typical phishing emails and contains more directed instructions and information. This attack is called spear phishing since the email was directed specifically to a single user with specific instructions. By clicking the link in the email, it exposed the computer to malware, or malicious software that infects a computer.

Here is an example of a phishing email:

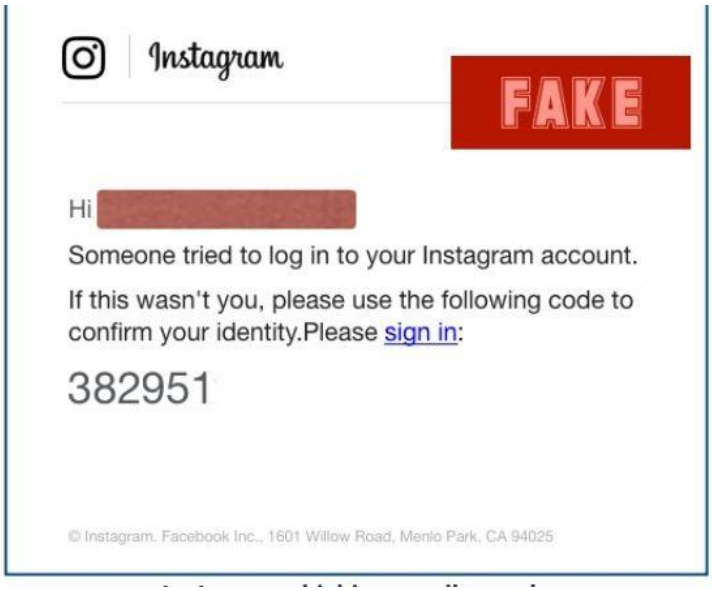


Image Source: Norton

This particular email might look credible since the logo is correct and text styling matches with other Instagram communications. In setting up 2-Factor Authentication (2FA) your code should be sent in a separate email before you have successfully logged in. You may also notice the lack of space between the last sentence. These are very small but detailed indicators that this email is fake!

- ❏ Take **5-10 minutes** review some of the examples of phishing emails on this website and see if you can identify the key details that it is a phishing attack.

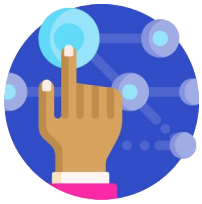
Phishing emails may be hard to detect. Here are some guidelines for determining if an email may be a scam.

- ➔ **Grammatical/Spelling Errors:** Are there grammatical errors in the message? Are some words misspelled or is the formatting slightly incorrect?
- ➔ **Logo/Image Errors:** Are images incorrect? Is it possible the sender is using an unofficial logo? Is the resolution, or image quality, low (are there fuzzy pixels)?
- ➔ **URL Errors:** Is a link different from the original/credible website? Perhaps the URL ends in .org instead of .com.

If you have identified a phishing email, here are some steps you can do to protect yourself from potential malicious attacks.

- ➔ **Do not click any links**. Phishing emails may click on links that install malware to your computers. Be sure to *never* click any of the links present in the email.
- ➔ **Report the email.** In many cases you should access the credible website in a new browser and notify the company of the suspicious email so that they can secure their websites. You should also report the email to the Federal Trade Commision at **ftc.gov/complaint**.
- ➔ **Never provide any personal information**. Phishing emails are meant to gather additional information from the users to make their systems more vulnerable. In many cases the hacker has yet to secure any information other than your email.
- ➔ **Change your password.** After an attack, it is good practice to change your passwords to secure your accounts just in case.

Step 5: Securing Your Online Footprint (5-10 mins)



Now that you have a small glimpse of some of the common cyber attacks, what is next?

- ➔ **Ensure your passwords are strong and secure.** Use a password manager like **BitWarden**, **KeePassXC**, or **LastPass** to keep track of your passwords and change them at least every 3 months.
- ➔ **Download antivirus/Malware software.** You may have malware on your computer already and do not know! Some free antivirus/malware software we suggest includes **Kaspersky**, **Avast**, **Malwarebytes**. Be sure to have this software run automatically so that you are checking your computer for malware often.
- ➔ **Always download the latest systems update.** Companies like Windows and Apple are always trying to ensure that the computers you use are secure. While updating your computers may take time, it is worth it since these updates often include preventative measures to protect your information.
- ➔ **Never share personal information.** You should be selective when sharing personal information, which may include your name, birthday, location, phone number, etc.. This information may not seem like much, but to a hacker getting a combination of this information may lead to receiving even more sensitive information like your social security number.
- ➔ **Educate others!** While many people may be aware of different cybersecurity threats, most people take few precautions to secure their computers. Share your knowledge of the importance of cybersecurity and how to secure computers and accounts with your friends and family.

Step 6: Extensions (5-30 mins)

Extension 1: Cybersecurity Fact of 2020 (5-10 mins)
As we think about how the internet connects us to people around the world, take a look at how hackers exploit this vulnerability in 2020. Read this **article** by CSO on different attacks this year! Also take note that this article was last published in March 2020 and the statistics may have changed since then!

Extension 2: Instagram Hacker Story (5-10 mins)
We wrote the story in this activity based on a real experience. You can see her original story **here**. Unfortunately, this situation happens all too often and on many social media platforms. You can also read about a similar experience in this Forbes **article**.

Extension 3: Learn more about other cyber attacks (10-30 mins)
In this activity we reviewed two types of cyber attacks, weak passwords and phishing attacks. Here are some resources to learn more about other cyber attacks that affect individuals and companies.

- ➔ **Scenario Based Student Guide** by CDSE
- ➔ **Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks** by Infocyte